ELECTRONIC AUTHENTICATION:

SUMMARY OF FINDINGS OF BILATERAL CONSULTATIONS

Prepared by:

ELECTRONIC COMMERCE TASK FORCE
INDUSTRY CANADA
OCTOBER 1999

EXECUTIVE SUMMARY

In October 1998, the Minister of Industry announced the details of the Government's cryptography policy. The policy envisaged, in certain categories of electronic transactions, the need for cryptographic technologies and related mechanisms that would provide for authentication, integrity and non-repudiation. The use of electronic authentication, and associated services provided by a trusted agent such as a certification authority (CA), can fulfil these transaction requirements. Canada's cryptography policy also states that the Government would not implement licensing regimes for CAs. Instead, the Government called for industry-led accreditation of CAs as a means of promoting sound business practices and building consumer confidence.

With a view to initiating discussion with potential CA service providers and other stakeholders to determine how authentication and certification services might evolve in Canada, the Electronic Commerce Task Force conducted a preliminary consultative program from May to October of this year. The objectives of this program were to:

i. consult with stakeholders to identify potential issues from the supplier and user perspectives;
ii. identify public policy considerations for governments;
iii. seek views on the respective roles of the private and public sectors; and,
iv. determine the need for more broadly based consultations.

A number of messages emerged from these preliminary discussions with stakeholders. On a general note, this process confirmed that there is a need for the public and private sectors to jointly discuss how authentication services should develop in Canada and their respective roles in the provision of them. More specifically, it would seem to be indicated that:

- the private sector agrees with the Government's decision to adopt a market-oriented approach to authentication and certification services in Canada but that the relative roles and responsibilities of the public/private sectors require further discussion;
- to achieve consumer confidence and effective business practices for CAs, there is a need to set minimum requirements, and possibly standards;
- public awareness and consumer education are critical to increasing the use of electronic authentication services;
- there is a need for federal/provincial harmony in approaches to authentication and certification services;
- active Canadian participation in the various international fora is essential to ensure compatible frameworks and prevent trade barriers; and,
- the public sector should facilitate ongoing public/private sector dialogue to continue to identify and further discuss issues requiring consideration and to explore, on a collaborative basis, options for addressing them.

Finally, it can be noted that, while there was broad consensus that these are very early days for this market and that much more experience is needed, all stakeholders expressed the view that the public/private sector information exchange and dialogue of the nature that Industry Canada has initiated is extremely important at this early stage, and will continue to be important as the market and the technology evolve.

BACKGROUND AND INTRODUCTION

On September 22, 1998, the Prime Minister announced Canada's Electronic Commerce Strategy and outlined various initiatives designed to establish Canada as a world leader in the adoption and use of electronic commerce. Working in close collaboration with the private sector, the Federal Government has concentrated on creating the most favourable environment possible in areas which are critical to the rapid development of electronic commerce.

While many strategic elements are being addressed (e.g., privacy, consumer protection), work is continuing on certain additional aspects such as authentication and certification services that are related to fostering user confidence and building trust in electronic markets.

This document provides a summary of the findings of an initial consultative program on consultation and certification services. The consultation involved a series of informal discussions with representatives of the private sector including suppliers of products and services, auditors/evaluators, business end users and consumer representatives as well as presentations at two workshops involving members of the Information Technology Association and one of its affiliates. Informal discussions were also held with some of the provinces known to be active in the area. A list of those who participated in the process is appended to this report.

SCOPE AND APPROACH

In this work, very general, high-level parameters are used to define authentication and certification services. They were necessarily at this level given that Industry Canada's interests lie predominantly in broad public policy aspects of authentication services, and less so at the detailed implementation level.

In its approach, Industry Canada recognizes that different kinds of transactions will require different kinds of solutions and that the choice of technology will be driven by the requirements of the parties involved. Further, there is recognition that levels of assurance or "gradations" of authentication would be implemented depending on the requirements of the application. As such, Industry Canada has adopted a technology-neutral approach to this work and has not focussed on any specific security solution.

In this series of meetings, stakeholder views on market developments, potential issues, private/public sector roles and responsibilities, and finally, possible next steps in the consultative process were sought. This report provides a summary of the input obtained in each of these areas followed by some conclusions about the messages emerging from these consultations.

MARKET DEVELOPMENT

While there are many ways to classify the various business models and environments in this market, predominantly there are three types differentiated on the basis of whether there is contractual privity amongst the parties. At this point, it is generally understood that "closed" models, where parties are bound by pre-existing contractual rules and procedures, lie at one end of this continuum. At the other end are Aopen@ models where parties communicate electronically without prior agreement. Hybrids lie on a continuum between the two extremes. Such hybrids essentially involve closed communities where the parties have additional bilateral and multilateral agreements that provide for digital certificates to be relied

upon by multiple parties. Intermediaries and third parties could also be introduced such that direct contractual agreements may not exist between the end parties.

Most of the literature makes a distinction between the models in this manner and the majority of countries have adopted approaches that differentiate the environments on this basis. Support for this approach was borne out domestically, with the majority of stakeholders consulted agreeing with both the need for the distinctions, and the general basis upon which they were being made. However, it was observed that the models essentially fell on a continuum with the distinctions between them often blurred. There may be challenges ahead in arriving at mutually exclusive definitions for the models if it is determined that there is a need to apply differing requirements to them.

Among those consulted, there was some suggestion that, for reasons associated with liability, the open model appears to offer a less viable business case than the closed (or variations of closed) model where risk can be contained. This was felt to be especially true in the case of open models performing authorization functions.[1] Instead, most stakeholders believed that there will be a proliferation of closed and hybrid models with a growing market for intermediaries and out sourcing arrangements. In this connection, it was observed that the authentication services market offered new business opportunities to some industry sectors since players not previously involved in certain aspects of electronic commerce would have the technology to offer new services and assume new roles.

While most agreed that public policy challenges and considerations are presented in open and hybrid models, there was a diversity of opinion on whether closed models might also present some public policy considerations. Specifically, while some felt that there were no public policy issues associated with closed models and believed they should be left to function entirely according to the contracts established by the transacting parties, consumer representatives and certain interest groups believed there could be problems with this approach. In particular, there was concern expressed with the potential for imbalances of power in contracts. It was also observed that, even in the case of closed models, where contracts already exist between the transacting parties, they would not necessarily cover new services such as those involving electronic authentication and certification. In the case of there being intermediaries, where multiple agreements will exist with responsibilities allocated across various organizations, it was noted that there will be a further array of legal issues, particularly where certificates containing authorizing information are involved. As such, there would appear to be general agreement that a range of legal questions exist relative to authentication and certification services even where contracts are being relied upon.

In terms of specific characteristics of the market, there was agreement that, while complete security solutions such as those offered through the use of public key cryptography techniques would be widely employed in the future, other, less costly solutions will be used in the meantime. This was felt to be particularly true in the case of small and medium-sized enterprises. Some emphasized that the payback for robust security implementations will be realized only through the revenue streams generated by the business applications they are applied to and that these would take time to roll out. On this basis security needs to be viewed as an enabler with incremental solutions being deployed. However, others expressed the view that the use of authentication services will bring with it an increase in the incidence of

---

[1] It was suggested that there was a need to distinguish between identity certificates and authorization certificates and that, for liability reasons, authorization certificates would not likely be issued in open models.

identity fraud making it necessary for businesses to use robust security arrangements in the nearer term for their own protection.
While views varied on the future direction of the technology, the majority believe the approaches could eventually involve a smart card. However, it was recognized that there will be questions relative to the number of cards users can be reasonably expected to carry, and the number of certificates residing on each they can be expected to manage. It was emphasized that such questions raise a host of policy and social issues that will need to be carefully explored (e.g., aspects related to multiple use of certificates, the use of common identifiers etc.). It was also recognized that these issues will be further complicated by the fact that use of the various technologies is not mutually exclusive and that an array of combinations is likely to exist.

There was general agreement that the biggest current and future market potential in this area lay in business-to-business applications with payments being the most important category of transaction. As such, the stakeholders believed there was a need for businesses to develop trust relationships with each other internationally and that developing a global framework for the formation of these trust relationships should be one of the main focuses for Canadian government activity given these relationships would probably require some support by governments. In this connection, the continued active involvement of the federal government in authentication initiatives such as that underway within the Organization for Economic Co-operation and Development (OECD) was felt to be essential.[2] It was generally observed that, while Canada may be a relatively small player, it was by no means an insignificant one, and, as such, did have the ability to shape and influence international directions.

Virtually all those consulted observed that the authentication and certification services market is nascent with few suppliers and limited competition. As such, stakeholders believed that if competition and innovation were to be fostered, market forces should be allowed to prevail. In this connection, there was strong endorsement for Industry Canada's technology-neutral approach and the decision to let the private sector take the lead. Some acknowledged that this approach could lead to a period of confusion in the market, with imperfections, but that this was preferable to trying to provide a framework early on in such a rapidly evolving market.

Potential Principles and Issues for Consideration

In its approach to authentication and certification services, Industry Canada has developed a set of principles to guide its work. This set of principles was used in these consultations and the following provides a summary of the issues identified by stakeholders in the context of each. For purposes of this report, the issues have been grouped under the relevant principle. However, their inter-related nature suggests that other frameworks for analysis may evolve in subsequent phases of these consultations.

For the most part, the issues of interest to the stakeholders did not vary according to their orientation (i.e., user, supplier etc.). Rather, with the exception of consumer end users whose interests were consistent across the business models, they seemed to vary by industry sector and depend on the nature of the

[2]The OECD published a "Ministerial Declaration on Authentication for Electronic Commerce" in October 1998 and in June 1999, convened a joint OECD/Private Sector Workshop on Electronic Authentication to exchange views on business models and global issues.

applications that would be deployed in that sector. On this basis, it would appear that, as this process moves forward, it will be important to keep in mind that the issues will differ in nature and priority across industry sectors and depend on the particular application involved. Thus, a flexible approach, rather than a "one size fits all" approach, would appear to be the most workable framework for the establishment of CA service providers in Canada.

While there was general agreement that the principles developed were useful in guiding the work at this stage, it was noted that they would require review on an ongoing basis and perhaps need to be revised in light of national or international market developments. It was also suggested that there may be a need to adjust the principles according to whether they were being applied to closed, open or hybrid environments. Some concerns were expressed about ensuring competition in all three models, particularly closed models. On this basis, there may be a need to refine the principles as we proceed.

1. Choice, Trust and Confidence: encourage competition

The elements embodied in this principle were viewed by most stakeholders as being the most important ones to address if electronic commerce was to flourish. With respect to the notion that choice must exist, consumer representatives believed that real choice would only be provided if open models proliferate. However, others observed that if this was to be the case, and as many suppliers as possible were encouraged to enter the market, issues related to consumer confusion and their ability to make informed choices would arise. In discussing ways to address these issues, some expressed the view that assurance seals could serve a useful function. Others were uncertain of their utility suggesting that assurance seals were of questionable value to consumers in this market and could easily be forged. It was suggested that some form of light regulatory approach that would ensure that CA operations would be required to meet minimum criteria related to aspects such as ease of use, reasonable cost, consumer protection measures etc. would be desirable. It was also felt that such an approach could address the extent to which a certification authority may use agreements to limit (or exempt) itself from losses resulting from the use of its certificates.

Given the general view that payment applications would be the driver in this market, there was also a message from both consumer and business users that choice in payment options would be important. Many expressed the view that there was a need for new payment types to emerge for this environment but some cautioned that their development should not be left to one industry sector as there were public policy issues at the design level (e.g., related to taking into consideration the needs of all parties in various aspects of the transaction, and not just the payment element) that will need to be addressed.

It was emphasized that all parties to transactions will need certainty with respect to their rights and responsibilities if trust and confidence in the environment is to be gained. In this connection, virtually all stakeholders believed that, regardless of the model, there was a need for full disclosure of the allocation of risks and liabilities of users, providers and third parties. Most did not offer specific suggestions on how this might be accomplished but did agree that it would be an important component of any public awareness campaign or user education program. However, some consumer representatives went further suggesting that there may be a need for consumer legislation (e.g., superseding legislation such as that which already exists in the marketplace) to guide the allocation of responsibilities in both open and closed models.

It was also noted that issues associated with the allocation of risks and liabilities across jurisdictions will need to be examined. On this basis, it was emphasized that the work underway in fora such as

"UNCITRAL" (United Nations Commission on International Trade Law) and the Internet Law Policy Forum to address some of these questions and related legal matters on a global basis was very useful.

Privacy was also identified as critical to instilling trust and confidence in the electronic marketplace. While it was acknowledged that Bill C-6 (formerly C-54, the *Personal Information Protection and Electronic Documents Act)* will provide a legal framework for the protection of personal information when it is passed, many believed the matter should be specifically addressed in the context of this work. In this regard, it was suggested that a principle related to the need for the development and application of authentication and certification services to be "privacy-respecting" or even "privacy-enhancing" may be required.

In the context of the discussion of this principle, there were views expressed about consumer expectations. Specifically, it was noted that consumer expectations will need to be managed as there appears to be a perception that electronic authentication affords the opportunity to enhance levels of consumer protection. It was suggested that consumer expectations in areas such as redress are likely to be very high. In exploring this topic, most stakeholders pointed out that discussions of "security" concerns with consumers had revealed that their concerns were not necessarily security-related but rather were concerns related to the components of traditional commerce transactions and how they are implemented in electronic commerce (e.g., refunds, assurance of product quality etc.). This suggests that there will be a need to carefully define and scope discussions of authentication and certification services as they proceed. Aspects not directly related to authentication services should be addressed in the appropriate fora.

2. Market Driven Development: private sector has lead role

While some stakeholders expressed full support for adopting a pure market approach, others believed that such an approach was too "hands off". Specifically, while they supported the notion of the private sector taking a lead role, they believed there was a need to ensure that industry proceeded within the context of broader policy frameworks. Others went further and suggested that there was a need for government to set some basic parameters for what makes a good CA and what makes it secure.

Regardless of the particular view as to the best approach, there was consensus that there was a need for the public and private sectors to work together toward a co-ordinated strategy for the development and use of authentication services in Canada. In this connection, it was observed that market forces alone cannot be relied upon if Canada is to meet its objective of becoming a world leader in this area. Some suggested that there was an immediate need for this process to begin or Canada would lose business opportunities.

3. Jobs and Growth in Canada: ensure a fair marketplace and no barriers to investment

There was a widely-held opinion that there will be competition issues to manage in this market as it evolves. It was observed that these issues will be wide-ranging in that they could be related to consumers (e.g., potential requirements that consumers are precluded from doing business with an organization unless they are "certified" by a particular CA) or to business users (e.g., small businesses precluded from procurement processes on the basis of the security technology they employ).

Again recognizing the likely predominance of payment transactions in this environment, virtually all stakeholders suggested that it would be important to recognize the very significant role the financial services sector would play in this market. In this connection, it was suggested that there was a need to

monitor the developments in this sector and address the public policy issues that could potentially arise there. In particular, it was suggested that competition issues associated with aspects related to market dominance, pricing of services, innovation etc., could arise. On a more general note, it was observed that CAs, and intermediaries offering CA services, would be taking on very powerful roles in the electronic commerce environment and that this needed to be recognized.

With respect to business and investment opportunities, the continued active involvement of Canada in the various international fora addressing authentication was viewed as critical to ensuring the global acceptance and use of Canadian products and services with no trade barriers.

4. Interoperable Infrastructures: the role of standards

There was a convergence of opinion on the role of standards in this environment. Specifically, most agreed that there was a consistent and coherent approach needed at both the national and international level, and that standards could play a role in this regard. It was felt that some form of "standards" were essential for cross-certification, and would facilitate the level of interoperability that users will expect, and that they would go a long way to establishing a level playing field for new products and services.

There was general agreement that it was too early to know what form these "standards" should take (e.g., code, norms, best practices statements etc.) and there were differing views on who should be responsible for their development. While the predominant view seemed to be that the market should take care of the need for standards, some suggested that there may be a need for government to set minimum requirements for the accreditation and verification of CAs upon which to base the standards. A minority view was that, for market efficiency reasons, the government should set the standards.

Most believed that international standards are of greatest importance given the global nature of electronic commerce but views varied on whether the approach should be to develop standards at the national level and progress them into the international fora, or to concentrate activity at the international level and work on a "top-down" basis. In the case of the former approach, many observed that, to date, Canada had already taken a lead role in many aspects of the electronic marketplace and had influenced international directions. Those making this suggestion believed that, if Canada wished to take a lead in this market, then rules for accreditation and verification of CAs in Canada should be established on a timely basis. They noted that adopting such a strategy would provide for cross-certification and interoperability across Canada. Others believed a broader approach was required and suggested that there may be a need for a North American framework along the lines of the European Union's (EU) proposal for a directive on a common framework for electronic signatures[3] and the work underway to develop standards and open specifications to underpin the requirements in that directive.[4]

---

[3] A European Parliament and Council Directive on a common framework for electronic signatures. Amended proposal: COM(1999) 195 final, 29.04.1999.

[4] The European Electronic Signature Standardization Initiative (EESSI) under the direction of a Steering Committee composed of industry experts, representatives of various industry groups and members of the European Commission.

There was a broad range of views on whether there was a need for third party verification of CA operations. While some were of the opinion that there was a definite need for some form of independent agency to perform such a role, others suggested that declarations of conformance to a set of standards, backed by penalties and liability for non-adherence, would be a better approach. Still others believed the marketplace would be the test and that businesses with inadequate or inferior implementations simply would not survive in the market.

5. Domestic Harmonization: compatible federal and provincial requirements

It was emphasized that an approach to authentication involving an array of requirements across the provinces would be inefficient and undesirable. It was felt that the Federal Government had a role to play in avoiding any such outcome and preventing the creation of provincial barriers in this market. However, it was acknowledged that, given the emerging nature of the market and the technology, it would take some time for federal and provincial roles to evolve. In discussing how a harmonized approach across jurisdictions could be achieved, some expressed concern that such processes often result in parameters being established at the level of the lowest common denominator and that this would not be the best result. As such, they believed there should be a strong effort to avoid this outcome.

6. Canadian Certificates Recognized Globally: compatibility with international directions

It was readily recognized that the challenge of harmonizing standards and accreditation approaches is not simply a domestic one. It was stressed that, given the global nature of electronic commerce, a "made in Canada" approach will not be the answer if we want to ensure that trade barriers are not created for Canadian consumers and businesses in other jurisdictions. As such, in the context of this principle, stakeholders again indicated that active Canadian participation in the various initiatives aimed at developing collaborative solutions across jurisdictions was critical. Some believed that there was more of a need to focus on North American initiatives than those at a more international level.

While stakeholders understood the evolving nature of these various initiatives, they believed improved communication about the work, its timing, the importance of Canada's involvement in it, and the need for consensus would facilitate the necessary "buy-in" from the business community at later stages.

ROLES AND RESPONSIBILITIES

Throughout these consultations, stakeholders expressed preliminary views on the potential roles and responsibilities of the public and private sectors in addressing the various issues and, for the most part, these are captured in the discussion above. However, messages related to roles and responsibilities for more general aspects also emerged. In particular, stakeholders stressed that the Federal Government had a very important role to play in terms of being a model user and suggested that it should move quickly to full-scale implementations of its various pilots and pathfinder projects. Some believed that, through this model user role, the Federal Government could provide the beginnings of a framework for the market, establishing a basis for further development by the private sector. Others added that this model user role should be exploited to a greater degree such that the federal government would actually stimulate and "incubate" the market.

It was also suggested that governments, both federal and provincial, had a role to play in increasing public awareness and providing user education. This was felt to be particularly true in the case of open models where the requirements would be greatest although specifics on the scope and nature of what this role should be were not offered.

Given the consensus that public and private sector collaboration is necessary in addressing many of the issues identified, it was felt that the Federal Government had an important role as a facilitator and catalyst to bring the various interests together. It was noted that it was very useful for government to "close the loop" in this process by distilling and feeding input back to all stakeholders via processes and reports such as this.

POTENTIAL NEXT STEPS

In discussions, stakeholders observed that there was a need to ensure that the potential issues that will require consideration are clearly articulated and well-understood by all parties. While they believed these preliminary consultations served a useful purpose in terms of beginning the dialogue and confirming the general nature of the issues, they felt subsequent phases of the process should involve discussions aimed at clearly defining the issues and perhaps prioritizing them. It was felt that only in this way, could the range of options and alternatives available to address the identified issues be discussed. It was suggested that bringing together the various industry sectors, providing for the blending of technical interests and business/policy issues, would be very important. In this regard, there was support expressed for convening a roundtable to further discuss the development and use of authentication and certification services in Canada.

Attachment

LIST OF STAKEHOLDERS CONSULTED : INDUSTRY CANADA PRELIMINARY CONSULTATIONS ON AUTHENTICATION

Academia (Univeristy of Ottawa)
Auditor General
BCE Emergis Inc.
British Columbia Technology Industries Association
Canada Post
Canadian Bankers Association
Canadian Direct Marketing Association
Canadian Federation of Independent Business
Canadian Health Coalition
Canadian Institute of Chartered Accountants
Canadian Payments Association
Consumers Association of Canada
DataPrivacy Partners Ltd.
Deloitte & Touche
Entrust Technologies
IBM Canada Limited
Information Technology Association of Canada
KPMG
Nortel Networks
Office of the Privacy Commissioner of Canada
Option consommateurs
Provinces (B.C., Ontario, Quebec)
Public Interest Advocacy Centre
Retail Council of Canada
Royal Bank
Sprint Canada

AUTHENTIFICATION ÉLECTRONIQUE :

CONSULTATIONS BILATÉRALES – SOMMAIRE DES CONCLUSIONS

Document préparé par le : GROUPE DE TRAVAIL SUR LE COMMERCE ÉLECTRONIQUE
INDUSTRIE CANADA
OCTOBRE 1999

RÉSUMÉ

En octobre 1998, le ministre de l'Industrie a annoncé les détails de la politique du gouvernement en matière de cryptographie, laquelle envisageait, dans certaines catégories d'opérations électroniques, la nécessité de faire appel à des techniques cryptographiques et à des mécanismes connexes qui répondraient aux exigences d'authentification, d'intégrité et de non-répudiation. Il est possible de répondre à ces exigences en recourant aux services d'authentification électronique et autres services connexes que fournit un agent de confiance, comme une autorité de certification (AC). La politique du Canada en matière de cryptographie dit qu'il ne mettrait pas en œuvre de régimes d'octroi de licences à l'intention des autorités de certification (AC). Il a plutôt proposé que ces dernières soient soumises à un processus d'accréditation mené par l'industrie, ce qui favoriserait l'établissement de saines pratiques commerciales et susciterait la confiance des clients.

Désireux de lancer le débat avec d'éventuels fournisseurs de services d'authentification et d'autres intervenants en vue de déterminer comment ce processus des services d'authentification et de certification mené par l'industrie pourrait prendre forme au Canada, le Groupe de travail sur le commerce électronique a réalisé un programme de consultations préliminaires de mai à octobre 1999. Les objectifs de ce programme étaient les suivants :

i. consulter les intervenants afin de relever les problèmes possibles du point de vue des fournisseurs et des utilisateurs;
ii. relever, à l'intention des gouvernements, diverses questions d'intérêt public;
iii. obtenir des idées sur les rôles respectifs du secteur privé et du secteur public;
iv. déterminer le besoin de procéder à des consultations plus larges.

Un certain nombre de points sont ressortis des discussions préliminaires avec les intervenants. D'un point de vue général, le processus a confirmé qu'il est nécessaire que le secteur public et le secteur privé discutent conjointement de la manière dont les services d'authentification devraient s'étendre au Canada, ainsi que de leurs rôles respectifs à l'égard de la prestation de ces services. Plus précisément, il semblerait que :

- le secteur privé soit d'accord avec la décision du gouvernement d'adopter, à l'égard des services d'authentification et de certification au Canada, une approche axée sur le marché; selon le secteur privé, les rôles et les responsabilités relatifs du secteur public et du secteur privé nécessiteraient toutefois de plus amples discussions;
- il soit nécessaire de fixer des exigences de base, voire des normes, afin de gagner la confiance des consommateurs et d'établir des pratiques commerciales efficaces pour les AC;
- la sensibilisation du public et l'information des consommateurs soient deux éléments indispensables à l'utilisation accrue des services d'authentification électroniques;
- il soit nécessaire d'harmoniser les approches fédérales et provinciales à l'égard des services d'authentification et de certification;

- il soit essentiel que le Canada participe de manière active aux diverses tribunes internationales afin de s'assurer que l'on établit des cadres compatibles et que l'on évite les obstacles au commerce;
- le secteur public doive faciliter la tenue d'un dialogue permanent entre le secteur public et le secteur privé afin de continuer de relever et d'analyser de manière approfondie les questions qui doivent être examinées, et de trouver, en collaboration, les options permettant de les régler.

Enfin, il faut mentionner que si les intervenants étaient généralement d'accord pour dire que ce marché est encore tout jeune et qu'il est nécessaire d'acquérir beaucoup plus d'expérience, tous étaient d'avis qu'un échange d'information et un dialogue entre le secteur public et le secteur privé, comme ce qu'Industrie Canada a entrepris, sont extrêmement importants à ce stade initial, et continueront de l'être à mesure qu'évolueront le marché et la technologie.

CONTEXTE ET INTRODUCTION

Le 22 septembre 1998, le premier ministre a annoncé la stratégie en matière de commerce électronique du Canada et exposé diverses initiatives conçues pour faire du pays un chef de file mondial sur le plan de l'adoption et de l'utilisation de cette forme de commerce. En collaboration étroite avec le secteur privé, le gouvernement fédéral s'est attaché à créer le milieu le plus propice qui soit dans des secteurs qui revêtent une importance cruciale pour l'expansion rapide du commerce électronique.

De nombreux éléments stratégiques seront examinés (comme le respect de la vie privée et la protection des consommateurs) mais, pour ce qui est de certains autres aspects liés au fait de susciter la confiance des utilisateurs à l'égard des marchés électroniques, tels les services d'authentification et de certification, le travail se poursuit.

Le présent document résume les conclusions de ce programme de consultations initiales, qui comportait une série de discussions non officielles avec des représentants du secteur privé. Y ont participé des fournisseurs de produits et de services, des vérificateurs/évaluateurs, des utilisateurs ultimes du secteur des affaires ainsi que des représentants des consommateurs. Dans le cadre du programme, il y a aussi eu des exposés présentés à l'occasion de deux ateliers auxquels ont participé des membres de l'Association de la technologie de l'information et de l'un de ses affiliés. Des discussions non officielles ont également eu lieu avec certaines des provinces reconnues comme très actives dans le domaine. Une liste des participants est présentée à la suite de ce rapport.

ÉTENDUE ET APPROCHE

Dans ce travail, nous utilisons des paramètres de haut niveau et de nature très générale pour définir les services d'authentification et de certification. En effet, Industrie Canada s'intéresse principalement aux aspects généraux, liés à l'intérêt public, des services d'authentification, et moins au niveau détaillé de leur mise en œuvre.

Dans son approche, Industrie Canada reconnaît que des types d'opérations différents nécessiteront des types de solutions différents, et que le choix de la technologie applicable dépendra des exigences des parties en cause. En outre, il est reconnu que l'on appliquera pour les services d'authentification divers degrés d'assurance ou « gradations », suivant les exigences de l'application utilisée. Dès lors, Industrie Canada a abordé ce travail sous un angle neutre d'un point de vue technologique, et n'a pas mis l'accent sur une solution de sécurité particulière.

Dans cette série de réunions, le Ministère a sollicité l'opinion des intervenants sur l'expansion du marché, les problèmes éventuels, les rôles et les responsabilités du secteur privé et du secteur public et, enfin, les

prochaines étapes possibles du processus de consultation. Le présent rapport résume les commentaires que nous avons obtenus pour chacun de ces volets, et présente ensuite quelques conclusions sur les grands points qui sont ressortis de ces consultations.

EXPANSION DU MARCHÉ

Il existe de nombreuses façons de classer les divers modèles et milieux d'affaires qui sont présents dans ce marché, mais trois types se différencient d'après l'existence – ou non – d'un lien de droit contractuel entre les parties. À ce stade-ci, il est généralement entendu que les modèles dits « fermés », dans lesquels les parties sont liées par des règles et des procédures contractuelles préexistantes, se trouvent à l'une des extrémités de ce continuum. À l'autre extrémité figurent les modèles dits « ouverts », dans lesquels les parties communiquent par voie électronique sans entente préalable. Entre ces deux extrêmes s'échelonnent une série de modèles hybrides, qui comprennent essentiellement des collectivités fermées dans lesquelles les parties sont dotées d'ententes bilatérales et multilatérales additionnelles prévoyant l'octroi de certificats numériques auxquels se fieront de multiples parties. Il pourrait également y avoir des intermédiaires et des tierces parties, ce qui signifie qu'il n'existerait peut-être pas d'ententes contractuelles directes entre les parties ultimes.

Dans la plupart des cas, c'est ainsi que la littérature spécialisée distingue les différents modèles, et la majorité des pays ont adopté des formules qui différencient les milieux de cette façon. C'est cette approche que l'on appuie à l'échelon national, et la majorité des intervenants consultés souscrivent à la fois à la nécessité de ces distinctions et au fondement général de ces dernières. Il a été signalé toutefois que les modèles se situent essentiellement le long d'un continuum au sein duquel les éléments qui les distinguent sont souvent flous. S'il s'avère nécessaire d'appliquer aux modèles des exigences différentes, on pourrait avoir de la difficulté à établir pour ces derniers des définitions mutuellement exclusives.

Certains des intervenants consultés ont laissé entendre que, pour des questions de responsabilité, le modèle ouvert semble représenter une solution moins viable que le modèle fermé (ou des variations de ce dernier), où il est possible de limiter les risques. Cela s'appliquerait spécialement aux modèles ouverts qui exécutent des fonctions d'autorisation.[1] La plupart des intervenants étaient plutôt d'avis que l'on assistera à une prolifération de modèles fermés et de modèles hybrides, et que le marché des intermédiaires et de l'impartition prendra de l'ampleur. À cet égard, il a été signalé que le marché des services d'authentification offrirait de nouveaux débouchés à certains secteurs de l'industrie car des intervenants, non liés antérieurement à certains aspects du commerce électronique, posséderaient la technologie requise pour offrir de nouveaux services et jouer de nouveaux rôles.

La plupart des intervenants ont convenu que les modèles ouverts et hybrides suscitent des défis et des questions d'intérêt public; quant à la question de savoir si les modèles fermés peuvent présenter eux aussi de telles questions, les opinions variaient. Plus précisément, si certains étaient d'avis qu'aucune question d'intérêt public n'était associée aux modèles fermés et croyaient qu'il faudrait laisser ces derniers fonctionner d'une manière entièrement conforme aux contrats établis par les parties en cause, les représentants des consommateurs et certains groupes d'intérêt ont indiqué que cette approche pourrait présenter des difficultés. Plus particulièrement, certains ont fait part de leur inquiétude à l'égard du risque que des contrats comportent des déséquilibres de pouvoir. Il a été souligné aussi que, même dans le cas des modèles fermés, qui comportent déjà des contrats entre les parties en cause, ceux-ci ne porteraient pas

---

[1] Il a été indiqué qu'il est nécessaire de faire la distinction entre les certificats d'identité et les certificats d'autorisation et que, pour des questions de responsabilité, dans les modèles ouverts on ne délivrerait probablement pas de certificats d'autorisation.

nécessairement sur de nouveaux services, comme ceux comportant des services de certification et d'authentification électroniques. Il a été ajouté que, dans les cas où des intermédiaires sont présents, c'est-à-dire lorsqu'il existe de multiples ententes dans le cadre desquelles les responsabilités sont réparties entre diverses organisations, il se posera une autre série de questions juridiques, plus particulièrement dans les situations où l'on aura affaire à des certificats comportant des informations d'autorisation. Dans ce contexte, il semble que l'on s'entende généralement pour dire que les services d'authentification et de certification suscitent une gamme de questions juridiques, et ce, même dans les cas où l'on se fie à des contrats.

En ce qui a trait aux caractéristiques précises du marché, les participants ont convenu qu'à l'avenir, on recourra dans une large mesure à des solutions de sécurité complètes, comme celles qu'offrent les techniques de cryptographie à clé publique, mais que l'on emploiera dans l'intervalle d'autres solutions moins coûteuses. Ils estiment que cela s'applique particulièrement aux petites et moyennes entreprises. Certains ont souligné que les mesures de sécurité solides que l'on implantera ne seront rentables que grâce aux sources de revenus générées par les applications commerciales auxquelles elles sont destinées, et qu'il faudra du temps pour les déployer. De ce fait, la sécurité doit être considérée comme un instrument d'appui auquel s'ajouteront des solutions supplémentaires. Cependant, d'autres ont exprimé l'avis que les services d'authentification s'accompagneront d'une intensification des cas de fraude en matière d'identité, ce qui obligera les entreprises à prendre à court terme des mesures de sécurité solides pour assurer leur propre protection.

Bien que les opinions varient quant à l'orientation future de la technologie, la majorité des intervenants croient que les solutions envisagées comprendront une carte à mémoire. Il a cependant été reconnu que des questions se poseront au sujet du nombre de cartes que l'on peut raisonnablement s'attendre à ce que les utilisateurs possèdent, ainsi qu'à propos du nombre de certificats implantés dans chacune des cartes qu'ils peuvent gérer. Il a été souligné que les questions de ce genre soulèvent une série de difficultés d'ordre social et politique, qu'il faudra soigneusement étudier (comme les aspects liés à l'usage multiple de certificats, l'utilisation d'identificateurs communs, etc.). Les intervenants ont également reconnu qu'à ces difficultés s'ajoutera le fait que l'emploi des diverses technologies n'est pas mutuellement exclusif, et qu'il y aura probablement une gamme de combinaisons possibles.

Les intervenants ont convenu de manière générale que, dans ce secteur, le potentiel de marché le plus intéressant, à l'heure actuelle et à l'avenir, réside dans les applications inter-entreprises et que les paiements constitueront la catégorie d'opérations la plus importante. Dans ce contexte, ils croient nécessaire que les entreprises nouent entre elles des liens de confiance à l'échelon international et ils estiment que l'établissement d'un cadre mondial favorisant la formation de ces liens de confiance devrait être l'un des principaux objectifs du gouvernement canadien, car ces liens nécessiteront probablement un certain appui de la part des gouvernements. À cet égard, il a été jugé essentiel que le gouvernement fédéral participe activement et de façon soutenue à des initiatives d'authentification comme celle entreprise par l'Organisation de coopération et de développement économiques (OCDE).[2] Les participants ont fait remarquer de manière générale que le Canada, même s'il est un intervenant d'une taille relativement petite, joue un rôle non négligeable et que, dans ce contexte, il est réellement en mesure de façonner et d'influencer les orientations qui seront prises à l'échelon international.

---

[2] En octobre 1998, l'OCDE a publié une déclaration ministérielle sur l'authentification pour le commerce électronique (« Ministerial Declaration on Authentication for Electronic Commerce ») et, en juin 1999, a tenu un atelier mixte (OCDE/secteur privé) sur l'authentification électronique en vue d'échanger des points de vue sur les modèles commerciaux et les problèmes mondiaux.

La quasi-totalité des intervenants consultés ont fait remarquer que le marché des services d'authentification et de certification est encore très jeune, que les fournisseurs sont rares et que la concurrence est restreinte. Dès lors, les intervenants croient que pour favoriser la concurrence et l'innovation il faudrait laisser jouer les forces du marché. Sur ce plan, les intervenants souscrivaient dans une large mesure à l'approche neutre adoptée par Industrie Canada en matière technologique ainsi qu'à la décision de laisser le secteur privé prendre les devants. Certains ont reconnu que cette démarche pouvait mener à une période de confusion au sein du marché, ainsi qu'à des imperfections, mais que cela valait mieux que d'essayer très tôt d'établir un cadre au sein d'un marché en évolution rapide.

PRINCIPES POSSIBLES ET QUESTIONS À CONSIDÉRER

L'approche d'Industrie Canada à l'égard des services d'authentification et de certification comporte une série de principes pour orienter le travail du Ministère. Cette série de principes a été utilisée dans les consultations, et ceux qui suivent présentent sous forme sommaire les points qu'ont relevés les intervenants dans le contexte de chacun des principes. Pour les besoins du présent rapport, les différents points ont été groupés sous le principe applicable. Toutefois, leur interdépendance dénote que d'autres cadres d'analyse pourraient se développer ultérieurement au cours de ces consultations.

En général, les questions qui intéressaient les intervenants ne dépendaient pas de l'orientation de ces derniers (utilisateur, fournisseur, etc.). Exception faite des consommateurs-utilisateursultimes, dont les intérêts étaient les mêmes dans tous les modèles commerciaux, les questions d'intérêt semblaient varier selon le secteur industriel et dépendre de la nature des applications qui y seraient déployées. Il semble ainsi que, au fur et à mesure que ce processus évoluera, il sera important de garder à l'esprit que la nature et la priorité des questions à considérer différeront d'un secteur industriel à un autre et dépendront de l'application particulière qui sera utilisée. Cela signifie donc que la solution la plus pratique pour l'établissement de fournisseurs de services d'authentification au Canada semble être une approche flexible, plutôt qu'une approche unique.

Les intervenants s'entendaient en général pour dire que les principes élaborés étaient utiles pour orienter le travail à ce stade-ci, mais on a signalé qu'il faudrait les examiner de façon permanente et, peut-être, les réviser en fonction de l'évolution du marché à l'échelon national ou international. Il a aussi été indiqué qu'il serait peut-être nécessaire de rajuster les principes selon qu'ils s'appliquent à un milieu fermé, ouvert ou hybride. Certains ont exprimé l'avis que l'on devrait veiller à ce qu'une certaine concurrence s'exerce dans les trois modèles, et surtout dans les modèles fermés. Il faudrait donc peut-être parfaire les principes au fur et à mesure que le travail progressera.

1. Choix et confiance : favoriser la concurrence

La plupart des intervenants ont considéré que les éléments de ce principe sont ceux à régler en priorité si l'on veut assurer le succès du commerce électronique. En ce qui concerne l'idée selon laquelle il doit y avoir du choix, les représentants des consommateurs croient que l'on n'offrira un véritable choix que si des modèles ouverts prolifèrent. Cependant, d'autres ont fait remarquer que si tel était le cas, et si l'on encourageait le plus de fournisseurs possible à se lancer dans le marché, cela créerait de la confusion chez les consommateurs et les empêcherait de faire des choix éclairés. En discutant des façons de régler ces difficultés, certains intervenants ont exprimé l'avis que des sceaux de garantie pourraient jouer un rôle utile. D'autres, incertains de l'utilité de ces sceaux, ont indiqué que ces derniers seraient d'une valeur douteuse pour les consommateurs au sein de ce marché et seraient faciles à contrefaire. D'aucuns ont indiqué qu'il serait souhaitable de recourir à une approche réglementaire légère, qui garantirait que les

activités d'authentification devraient satisfaire à des critères de base liés à divers aspects (facilité d'utilisation, coût raisonnable, mesures de protection des consommateurs, etc.). Certains croyaient aussi qu'une telle démarche pourrait régler la question de la mesure dans laquelle une autorité de certification pourrait se servir d'ententes pour limiter sa responsabilité vis-à-vis des pertes découlant de l'utilisation de ses certificats, voire le dégager de cette responsabilité.

Comme les intervenants étaient généralement d'avis que les applications de paiement seraient l'élément moteur de ce marché, les représentants des consommateurs et des entreprises ont également indiqué qu'il serait important d'offrir un certain choix en ce qui a trait aux options de paiement. Nombreux sont ceux qui ont indiqué de voir apparaître nouveaux types de paiement dans ce milieu, mais certains ont averti qu'il ne faudrait pas laisser la responsabilité de l'établissement de ces types de paiement aux soins d'un secteur industriel unique car il y aurait des questions d'intérêt public à régler au niveau conceptuel (des questions liées, par exemple, au fait de prendre en compte les besoins de toutes les parties dans divers aspects de l'opération, et non seulement dans l'élément « paiement »).

Il a été souligné que si l'on veut que le milieu inspire confiance, toutes les parties aux opérations devront avoir des certitudes en ce qui a trait à leurs droits et à leurs responsabilités. À cet égard, la quasi-totalité des intervenants ont exprimé l'avis que, peu importe le modèle, il était nécessaire de divulguer pleinement la part de risques et de responsabilités des utilisateurs, des fournisseurs et des tierces parties. La plupart des intervenants n'ont offert aucune suggestion précise quant à la façon d'atteindre cet objectif, mais ils ont quand même convenu qu'il s'agirait là d'un aspect important de n'importe quelle campagne de sensibilisation du public ou de n'importe quel programme d'information des utilisateurs. Toutefois, quelques représentants des consommateurs sont allés plus loin et ont laissé entendre qu'il serait peut-être nécessaire d'établir des dispositions législatives concernant les consommateurs (par exemple, des dispositions qui remplaceraient celles qui existent déjà au sein du marché) afin de guider l'attribution des responsabilités dans les modèles ouverts et les modèles fermés.

Il a été signalé par ailleurs qu'il sera nécessaire d'examiner la question de l'attribution des risques et des responsabilités entre les diverses administrations. On a ainsi été souligné l'utilité des travaux qui sont en cours au sein d'organismes tels que le CNUDCI (Commission des Nations Unies pour le droit commercial international) et l'*Internet Law Policy Forum* en vue de régler certaines de ces aspects ainsi que des questions juridiques connexes à l'échelon mondial.

Le respect de la vie privée est lui aussi un aspect crucial pour que le marché électronique puisse inspirer confiance. Si tous reconnaissent que le projet de loi C-6 (précédemment numéroté C-54 - *Loi sur la protection des renseignements personnels et les documents électroniques*) constituera, lorsqu'il sera adopté, un cadre juridique pour la protection des renseignements personnels, nombreux sont ceux qui croient qu'il faudrait traiter expressément de la question dans le cadre du présent travail. À ce sujet, on a indiqué qu'il faudrait peut-être élaborer un principe lié à la nécessité de faire en sorte que l'établissement et l'application des services d'authentification et de certification respectent, voire améliorent, la vie privée.

Dans le cadre des discussions relatives à ce principe, certains ont traité de la question des attentes des consommateurs. Plus précisément, on a signalé la nécessité de gérer ces attentes car certains pensent que l'authentification électronique offre la possibilité d'améliorer les niveaux de protection des consommateurs. On a ainsi suggéré que, dans des secteurs comme celui des recours, les consommateurs ont de très grandes attentes. En analysant le sujet, la plupart des intervenants ont fait remarquer qu'il était ressorti des discussions menées avec des consommateurs à propos de la « sécurité » que les préoccupations de ces

derniers n'étaient pas nécessairement liées à la sécurité mais plutôt à des éléments des opérations commerciales ordinaires et à la façon dont ceux-ci sont mis en œuvre dans le commerce électronique (les remboursements, les garanties de qualité de produits, etc.). Cela donne à penser qu'il sera nécessaire de cerner et de définir soigneusement les discussions relatives aux services d'authentification et de certification à mesure de leur déroulement. Les questions ne concernant pas directement les services d'authentification devraient être étudiées au sein des tribunes appropriées.

2. ***Expansion menée par le marché : le rôle de chef de file du secteur privé***

Quelques intervenants ont indiqué qu'ils appuyaient sans réserve l'idée d'adopter une approche fondée exclusivement sur le marché, mais d'autres croyaient qu'une telle démarche était trop « non interventionniste ». Plus précisément, tout en étant favorables à l'idée que le secteur privé joue un rôle de chef de file, ils estimaient qu'il faudrait veiller à ce que l'action de l'industrie soit soumise à des cadres de politique plus larges. D'autres sont allés plus loin et ont indiqué qu'il était nécessaire que le gouvernement détermine, à l'aide de quelques paramètres de base, ce qui constitue une bonne AC et ce qui fait que cette dernière est sûre.

Quels que soient les points de vue particuliers au sujet de la meilleure approche à suivre, les participants ont été unanimes à juger qu'il fallait que le secteur public et le secteur privé unissent leurs efforts pour établir une stratégie coordonnée à l'égard de l'implantation et de l'utilisation de services d'authentification au Canada. À cet égard, plusieurs d'entre eux ont souligné que le Canada ne devait pas se fier uniquement aux forces du marché s'il voulait atteindre son objectif de devenir un chef de file mondial dans ce domaine. Selon certains, ce processus devrait commencer sur-le-champ, faute de quoi le Canada perdrait des possibilités d'affaires.

3. ***Emplois et croissance au Canada : garantir un marché équitable et l'absence d'obstacles à l'investissement***

Les participants étaient généralement d'avis qu'à mesure que ce marché prendra de l'ampleur, il y aura des questions de concurrence à gérer. Ces questions seront d'une grande portée, en ce sens qu'elles pourraient être liées aux consommateurs (par exemple, on pourrait exiger que seuls les consommateurs « certifiés » par une AC particulière peuvent faire affaire avec une organisation déterminée) ou aux entreprises (par exemple, de petites entreprises ne pourraient prendre part à des processus d'approvisionnement à cause de la technologie de sécurité qu'elles utilisent).

Reconnaissant là encore la prédominance probable des opérations de paiement dans ce milieu, la quasi-totalité des intervenants ont indiqué qu'il serait important de tenir compte du rôle marquant que jouerait, au sein de ce marché, le secteur des services financiers. À cet égard, on a souligné la nécessité de surveiller l'évolution de la situation dans ce secteur et de régler les questions d'intérêt public qui pourraient y survenir. Plus particulièrement, on a indiqué la possibilité que surgissent des questions de concurrence associées à des aspects liés à la domination du marché, à la fixation des prix des services, à l'innovation, etc. D'un point de vue plus général, il a été noté que les AC et les intermédiaires offrant des services d'AC joueraient des rôles de tout premier plan dans l'univers du commerce électronique, et qu'il était nécessaire de reconnaître ce fait.

Au sujet des possibilités d'affaires et d'investissement, les intervenants ont considéré qu'il était indispensable que le Canada joue un rôle actif et soutenu dans les diverses tribunes internationales qui

s'occupent de la question de l'authentification, afin de garantir l'acceptation et l'utilisation, à l'échelon mondial, des produits et services canadiens, sans entraves au commerce.

4. *Infrastructures interopérables : le rôle des normes*

Nous avons relevé une convergence d'opinions à propos du rôle des normes dans ce milieu. Plus précisément, la plupart des intervenants ont convenu qu'il était nécessaire de suivre une démarche cohérente et uniforme à l'échelon national et international, et qu'à cet égard, les normes pourraient s'avérer importantes. Ils ont considéré qu'une certaine forme de « normalisation » était essentielle à la transcertification, qu'elle faciliterait le degré d'interopérabilité auquel s'attendent les utilisateurs et qu'elle contribuerait à uniformiser les règles du jeu pour les nouveaux produits et services.

Les participants ont convenu de manière générale qu'il était trop tôt pour savoir quelle forme devraient revêtir ces « normes » (code, normes, énoncés de pratiques exemplaires, etc.). La question de savoir qui devrait être chargé de leur élaboration a donné lieu à des points de vue différents. S'il a surtout semblé que c'était le marché qui devrait répondre au besoin d'élaborer des normes, certains ont déclaré qu'il serait peut-être nécessaire que le gouvernement fixe, au sujet de l'accréditation et de la vérification des AC, des exigences minimales sur lesquelles les normes seraient fondées. Selon une minorité, c'est le gouvernement qui devrait fixer les normes, et ce, pour des motifs liés à l'efficacité du marché.

La plupart ont exprimé l'avis que les normes internationales sont celles qui importent le plus, vu le caractère mondial du commerce électronique, mais les points de vue variaient au sujet de la question de savoir s'il conviendrait d'établir d'abord des normes à l'échelon national et de les soumettre ensuite aux tribunes internationales, ou de concentrer plutôt les activités à l'échelon international et de procéder ensuite du haut vers le bas. En ce qui concerne la première approche, de nombreux participants ont fait remarquer qu'à ce jour, le Canada joue déjà un rôle de chef de file dans de multiples aspects du marché électronique et qu'il a exercé une influence sur les orientations prises à l'échelon international. Les auteurs de cette remarque croient que si le Canada tient à jouer un tel rôle au sein de ce marché, il faudrait établir en temps opportun des règles concernant l'accréditation et la vérification des AC. Ils ont ajouté qu'une telle stratégie assurerait la transcertification et l'interopérabilité d'un bout à l'autre du Canada. D'autres ont exprimé l'avis qu'il était nécessaire d'adopter une approche plus large et ont indiqué qu'il faudrait peut-être établir un cadre nord-américain, qui refléterait la proposition de l'Union européenne (UE) concernant l'élaboration d'une directive sur l'établissement d'un cadre commun pour les signatures électroniques[3], ainsi que les travaux actuellement en cours pour élaborer des normes et des spécifications ouvertes sous-tendant les exigences que comporte cette directive.[4]

Les participants ont fait état d'une vaste gamme de points de vue au sujet de la nécessité qu'une tierce partie vérifie les activités des AC. Selon certains, il est bel et bien nécessaire qu'un organisme indépendant

---

[3] Directive du Conseil européen et du Parlement européen sur un cadre commun pour les signatures électroniques. Proposition modifiée : COM(1999) 195 (déf.), 29.04.1999.

[4] L'initiative européenne de standardisation des signatures électroniques (IESSE), sous la direction d'un comité directeur composé de spécialistes de l'industrie, de représentants de divers groupes industriels ainsi que de membres de la Commission européenne.

exécute une telle fonction, mais d'autres ont indiqué que des déclarations de conformité à une série de normes, soutenues par des pénalités et une responsabilité en cas de non-conformité, seraient une meilleure solution. D'autres encore croyaient que le marché constituerait le meilleur critère, et que les entreprises dont les applications seraient inadéquates ou de qualité inférieure ne pourraient tout simplement pas survivre.

5. ***Harmonisation nationale : compatibilité des exigences fédérales et provinciales***

Il a été souligné qu'il serait inefficace et peu souhaitable de recourir à une solution d'authentification qui comporte une gamme d'exigences différentes d'une province à une autre. Selon les participants, le gouvernement fédéral a un rôle à jouer pour éviter que cela se produise, ainsi que pour empêcher que l'on crée des obstacles provinciaux au sein de ce marché. Il a toutefois été reconnu qu'en raison de la nouveauté du marché et de la technologie, il faudra un certain temps avant que le rôle du gouvernement fédéral et celui des provinces ne soit défini.

Lors des discussions sur la façon d'obtenir une approche harmonisée entre les diverses administrations, certains ont exprimé leur inquiétude quant au fait que de tels processus amènent souvent à fixer des paramètres au niveau du dénominateur commun le plus bas, ce qui n'est le meilleur résultat. Dans cet esprit, ils étaient d'avis qu'il faudrait faire de gros efforts pour éviter un tel résultat.

6. ***Reconnaissance mondiale des certificats canadiens : compatibilité avec les orientations internationales***

Les participants ont tout de suite reconnu que le défi posé par l'harmonisation des normes et des méthodes d'accréditation ne se limite pas à l'échelon national. Ils ont souligné qu'en raison du caractère mondial du commerce électronique, une solution « fabriquée au Canada » ne sera pas la réponse appropriée si l'on veut s'assurer de ne pas créer dans d'autres administrations des obstacles commerciaux pour les consommateurs et les entreprises du Canada. Dans le contexte de ce principe, les intervenants ont réitéré qu'il était indispensable que le Canada participe de manière active aux diverses initiatives qui visent à trouver des solutions de collaboration entre les diverses administrations en cause. Selon certains, il importe davantage de se concentrer sur les initiatives nord-américaines que sur celles qui sont d'une envergure plus internationale.

Les intervenants étaient conscients du caractère évolutif de ces diverses initiatives, mais ils étaient d'avis que de meilleures communications concernant le travail accompli, le moment où ce dernier est effectué, l'importance de la participation du Canada à ce travail ainsi que la nécessité d'un consensus permettraient d'obtenir plus facilement l'« adhésion » nécessaire du milieu des affaires à un stade ultérieur.

RÔLES ET RESPONSABILITÉS

Pendant toute la durée de ces consultations, les intervenants ont fait part de points de vue préliminaires sur les rôles et les responsabilités que pourraient assumer le secteur public et le secteur privé à l'égard des divers enjeux, et la plupart de ces points de vue se retrouvent dans l'exposé qui précède. Cependant, il est ressorti aussi divers messages liés aux rôles et aux responsabilités concernant des aspects plus généraux. En particulier, les intervenants ont souligné que le gouvernement fédéral avait un rôle très important à jouer en tant qu'utilisateur modèle, et ils ont indiqué que ce dernier devrait entreprendre rapidement la mise en œuvre à grande échelle de ses divers projets pilotes et d'orientation. Certains ont indiqué que, grâce à ce

rôle d'utilisateur modèle, le gouvernement fédéral pourrait fournir les premiers éléments d'un cadre relatif au marché, qui servirait ainsi de base au secteur privé. D'autres ont ajouté qu'il faudrait exploiter davantage ce rôle d'utilisateur modèle, et que le gouvernement fédéral stimulerait et « incuberait » en fait le marché.

Il a été indiqué aussi que les gouvernements, tant fédéral que provinciaux, ont pour tâche de sensibiliser davantage le public et d'informer les utilisateurs. Cela, a-t-il été jugé, s'applique surtout aux modèles ouverts, où les exigences seraient les plus importantes, encore que l'on n'ait pas fourni de détails sur ce que devraient être l'étendue et la nature de ce rôle.

Compte tenu du consensus selon lequel il est nécessaire que le secteur public et le secteur privé collaborent pour régler un grand nombre des problèmes relevés, il a été jugé que le gouvernement fédéral avait un important rôle de facilitateur et de catalyseur à jouer sur le plan du rapprochement des divers intérêts. Il a été signalé qu'il serait très utile que le gouvernement « ferme la boucle » dans ce processus en filtrant les commentaires formulés et en les rétrodiffusant à tous les intervenants grâce à des processus et à des rapports comme celui-ci.

LES PROCHAINES ÉTAPES POSSIBLES

Lors des discussions, les intervenants ont fait remarquer qu'il fallait s'assurer que toutes les parties comprennent bien et exposent clairement les questions qui devront éventuellement être examinées. Ils étaient d'avis que ces consultations préliminaires jouaient un rôle utile pour ce qui était d'entamer le dialogue et de confirmer la nature générale des questions à étudier, mais ils ont toutefois considéré que les étapes suivantes du processus devraient comporter des discussions visant à définir clairement les enjeux et, peut-être, à les classer par priorité. Ce n'est que de cette façon, ont-ils considéré, que l'on pourrait discuter de la gamme d'options et de solutions de rechange disponibles pour régler les questions relevées. Il a été ajouté qu'il serait fort important de réunir les divers secteurs industriels, ce qui permettrait de combiner les intérêts techniques et les questions de principe ou d'affaires. À cet égard, les intervenants ont appuyé l'idée de tenir une table ronde afin de discuter plus avant de l'implantation et de l'utilisation des services d'authentification et de certification au Canada.

Pièce jointe

LISTE DES INTERVENANTS CONSULTÉS :
CONSULTATIONS PRÉLIMINAIRES D'INDUSTRIE CANADA SUR L'AUTHENTIFICATION

Association canadienne de la technologie de l'information
Association canadienne des paiements
Association canadienne du marketing direct
Association des banquiers canadiens
Association des consommateurs du Canada
Banque Royale
BCE Emergis Inc.
British Columbia Technology Industries Association
Centre pour la promotion de l'intérêt public
Coalition canadienne de la santé
Commissariat à la protection de la vie privée du Canada
Conseil canadien du commerce de détail
DataPrivacy Partners Ltd.
Deloitte & Touche
Entrust Technologies
Fédération canadienne de l'entreprise indépendante
IBM Canada Limitée
Institut canadien des comptables agréés
KPMG
Milieu universitaire (Université d'Ottawa)
Nortel Networks
Option consommateurs
Provinces (C.-B., Ontario, Québec)
Société canadienne des postes
Sprint Canada
Vérificateur général

Octobre 1999